What is a Complex Password

05/19/2004

Hackers sometimes use automated systems capable of attempting many thousands of passwords in a short period of time. If a complex password is not used, then those trying such "brute force" password guessing routines can fairly easily break into an account. So what is a complex password? By definition, a complex password meets the following requirements:

1. Cannot contain any or all of the user's name.
2. Must be at least 8 characters.
3. Must contain characters from 3 of the following categories.
    a. Uppercase English letters, (A to Z)
    b. Lowercase English letters, (a to z)
    c. Number 0 to 9
    d. Non-alphanumeric characters, (!, @, #, $, etc.)

To protect your password:

- Don't use the same password for all systems, in particular don't use the same password with a connection method that does not encrypt passwords as with one that does encrypt passwords.
- Don't write your password down.
- Change your password every 90 days.
- Use a unique password every time you change it.

Another idea is to use a lengthy password, since most password cracking tools assume the password will never exceed 14 characters, which is the limit that DOS network boot disks, Microsoft Remote Installation Services (RIS) Pre eXecutable Environment (PXE) boot disks, and older Lan Manager clients (Win9x) must utilize. Even without complexity, a very long password (>14 characters, up to 128 characters) can be the best possible protection against having an especially sensitive password hacked.

For instance, you might decide to use a long sentence that is easy to remember, e.g. “You can try and crack this until the cows come home”. Even if more than 14 characters is attempted, the length of this password alone makes the hacker’s task exponentially difficult.

If administrators have legacy systems, RIS, or similar requirements that stick to the 14 character passwords, or simply dislike dealing with an especially lengthy password, (fearing too many typos and lockouts might inadvertently occur) using a shorter password with complex characters offers good protection. However, keep in mind the longer the password the more difficult it is to crack. Adding both complexity *and* length makes it the most difficult of all to crack.

Examples

C0MP13Xp@$$w0rds – complex passwords

C@t&M0u$e – cat and mouse

Msi8Y0ld – My son is 8 years old

@t1Br@ves – Atlanta Braves

g00ds3cur!tE – good security

IG3T0ff@5 – I get off at 5

AUT1G3R$ – Auburn Tigers

9@meC0cks – GameCocks